WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Monday, December 29, 2003

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ	
☐	L11	('6618389')!.ABPN1,NRPN,PN,TBAN,WKU.	2
☐	L10	('20030212926')!.ABPN1,NRPN,PN,TBAN,WKU.	1
		DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ	
☐	L9	(('20030198186') [ABPN1,NRPN,PN,TBAN,WKU]) and @pd > 20031102	0
☐	L8	(('6618389') [ABPN1,NRPN,PN,TBAN,WKU]) and @pd > 20031102	0
☐	L7	(('20020172158') [ABPN1,NRPN,PN,TBAN,WKU]) and @pd > 20031102	0
☐	L6	(L3 and (communication or network)with (test$3 or inspect$4 or check$4 or debug$4 or verif$7 or diagno$5)near2 (delay$3 or late$4) same (traffic or agent) same (packet or frame) same (application or server or client or computer)) and @pd > 20031102	0
☐	L5	(('20020133575') [ABPN1,NRPN,PN,TBAN,WKU]) and @pd > 20031102	0
☐	L4	(L3 and (communication or network)with (test$3 or inspect$4 or check$4 or debug$4 or verif$7 or diagno$5) same (traffic with agent) same (delay$3 or late$4) same (packet or frame) same (application or server or client or computer)) and @pd > 20031102	1
☐	L3	(L2 and (communication or network)with (test$3 or inspect$4 or check$4 or debug$4 or verif$7 or diagno$5) same (traffic or agent) same (delay$3 or late$4) same (packet or frame) same (application or server or client or computer)) and @pd > 20031102	8
☐	L2	(L1 and (communication or network)with (test$3 or inspect$4 or check$4 or debug$4 or verif$7 or diagno$5) same (traffic or agent) same (delay$3 or late$4) same (packet or frame)) and @pd > 20031102	13
☐	L1	((communication or network)with (test$3 or inspect$4 or check$4 or debug$4 or verif$7 or diagno$5) same (traffic or agent) same (delay$3 or late$4)) and @pd > 20031102	23

END OF SEARCH HISTORY

L3: Entry 8 of 8 File: USPT Sep 9, 2003

DOCUMENT-IDENTIFIER: US 6618389 B2
TITLE: Validation of call processing network performance

Abstract Text (1):
A call processing network performance verification and validation system and test methodology. The call processing network implements Internet Protocol (IP) subnet topology, ATM WAN configuration, equipment placement, and device configuration to provide partitioning of a call processing application across multiple sites. The partitioning reduces latency for mission critical messages, while providing for necessary provisioning traffic needs. Further, the overall topology provides the redundancy and resiliency necessary for mission critical call processing application, utilizing the IP subnets, ATM permanent virtual circuits, network device configuration, and server segregation to achieve Quality of Service (QoS). The validation testing method and system proves out the various segregated routes, verifies subnet integrity and measures total latency and data path traversal in a verifiable manner.

DATE ISSUED (1):
20030909

Brief Summary Text (10):
Thus, in accordance with the invention, there is provided a system and method for validating a telecommunications call processing network comprising: a call processing network including a variety of application servers and network devices for simulating handling of call processing traffic along first segregated routes comprising one or more subnets between associated network devices, and handling of call provisioning traffic along second segregated routes comprising one or more subnets, the first and second segregated routes segregated according to call traffic latency requirements; test tool capable of communicating test information packets along selected segregated routes in the call processing network; and a mechanism for measuring round trip latencies of communicated packets along the selected segregated routes, whereby internetwork and intranetwork latency and subnet integrity for simulated packet traffic is verified.

Detailed Description Text (34):
As will be further described herein, for more complex testing, the NPT tool runs test suites including scripts which may send the packet through a sequence of systems and back, allowing for the computation of round trip delays for the network along an application communication path. Furthermore, an additional script may be added to the test suite that performs a traceroute to every interface address and hostname. The purpose of this demonstrates that the host files and routers are correctly set up, and that packets between specific systems followed the correct paths. Packets are only transmitted via an interface's primary address, the secondary address is used only for receiving packets. This means that, for instance, real-time subnet 2 traffic e.g., from the ATS, may be sent via the subnet 3 provisioning interface. Analysis of the output of this script from each system is used to validate the router configurations.

Detailed Description Text (47):
As mentioned above, a critical benchmark test includes the Path Validation & Latency Measurements test. According to the invention, the following tests are configured to ensure that traffic uses the intended network paths: a) CS-CPFR-TS which verifies basic Communications Server (CS) to Transaction Server (TS) connectivity path through the Call Processing FDDI Ring (CPFR) such as illustrated in FIG. 5(a). As the underlying technology is reliable and mature, this test is for latency data; b)

a CS-CPFR-TS-CPFR-ATS test which verifies performance of the connectivity path from CS to TS over subnet 1, and then from TS to the ATS via subnet 2, such as illustrated in FIG. 6(a); c) a CS-CPFR-TS-CPFR-ATS-CPFR-GDS (local) test which verifies performance of the communications path from the CS to the local GDS, such as shown in FIG. 7(a); d) a CS-CPFR-TS-CPFR-ATS-CPFR-Cisco 7513 FDDI-Cisco 7513 ATM-BPX-BPX-Cisco 7513 ATM-Cisco 7513 FDDI-CPFR-GDS (remote) test which verifies performance of the worst case real time connectivity path to a remote GDS such as shown in FIG. 8(a); e) a TS-PFR-GIGAswitch-SS test which verifies performance of the connectivity path from the TS to the SS via the PFR and GIGAswitch such as shown in FIG. 9(a), and which configuration may be considered identical to that using an ATS from a network point of view; f) a FEDS-GIGAswitch-Cisco 7513-BPX-BPX-Cisco 7513-GIGAswitch -BEDS test which verifies performance of the connectivity path from the FEDS across WAN path to the distant FEDS, such as illustrated in FIG. 10(a); g) a SS-GIGAswitch-Cisco 7513-BPX-BPX-Cisco 7513-GIGAswitch-RS test which verifies performance of the connectivity path from the SS to RS path across the WAN such as shown in FIG. 11(a); h) a LAN High Load R/T test for verifying the impact of flooding the Call Processing LAN with real-time traffic; i) a LAN High Load Provisioning test for verifying the impact of flooding the Provisioning LAN with provisioning traffic; j) a WAN High Load R/T test for verifying the impact of flooding the WAN with real-time traffic; k) a WAN High Load Provisioning test for verifying the impact of flooding the WAN with real-time traffic; and, l) a WAN High Load SS-RS test for verifying the impact of flooding the WAN with SS-RS traffic.

Detailed Description Text (70):
As mentioned above, a critical benchmark test includes the failover/failback tests for determining failover and failback times for each single component failure. The configuration for these sets of tests are similar to the benchmark topology for the LAN path and latency tests. In the LAN path and latency tests, the goal was to check if the traffic was using the expected routes. In the failover and failback tests, the aim is to measure failover times for each communications component. Successful failover/failback criteria are based on parameters including response times (before, during, and after failover), failover time to backup device, failback times from failback device to newly recovered primary device. Additionally, the effect on link status and routing may be monitored. Absolute success is determined by the observed data. For example, failover recovery times exceeding two (2) seconds is deemed excessive. Any detrimental effect on LAN/WAN routing capability, e.g., the inducement of unacceptable routes in failure recovery attempts, is additionally deemed unacceptable.

CLAIMS:

1. A system for validating a telecommunications call processing network comprising: a call processing network including a variety of application servers and network devices for simulating handling of call processing traffic along first segregated routes comprising one or more subnets between associated network devices, and handling of call provisioning traffic along second segregated routes comprising one or more subnets; said first and second segregated routes segregated according to call traffic latency requirements, and test tool capable of communicating test information packets along selected segregated routes in said call processing network; and mechanism for measuring round trip latencies of communicated packets along said selected segregated routes, whereby internetwork and intranetwork latency and subnet integrity for simulated packet traffic is verified.

15. A method for validating a telecommunications call processing network comprising the steps of: interconnecting a variety of application servers and network devices for simulating a call processing network capable of handling call processing traffic along first segregated routes comprising one or more subnets between associated network devices, and handling of call provisioning traffic along second segregated routes comprising one or more subnets; said first and second segregated routes segregated according to call traffic latency requirements, communicating test information packets along selected segregated routes in said call processing network; and measuring round trip latencies of communicated packets along said selected segregated routes, whereby internetwork and intranetwork latency and subnet integrity for simulated packet traffic is verified.